

**AFFIDAVIT OF JASON J. DEFREITAS IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason J. DeFreitas, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security (“DHS”) United States Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”) assigned to the Boston Field Office and have been employed by HSI since 2006. I am currently assigned to the Cyber Group. Prior to my assignment to the Boston Field Office, I was assigned to the HSI Los Angeles Field Office, where I served as a member of the Intellectual Property Rights Group. In connection with my official duties, I have investigated and assisted other agents in investigating cases involving a wide variety of criminal violations including, but not limited to, fraud, intellectual property rights, cultural property theft, and child pornography. Prior to my employment with ICE HSI, I served as a United States Customs and Border Protection (“CBP”) officer at the Los Angeles International Airport for approximately four years. My duties included the interception and examination of individuals and merchandise for violations of United States laws.

2. I submit this Affidavit in support of the following applications:

- a. Application under Rule 41 of the Federal Rules of Criminal Procedure to search the residence located at 12 Clifton Street, Fitchburg, Massachusetts 01420 (the “SUBJECT PREMISES”) and the person of Ryan Decarolis (YOB 1993). The SUBJECT PREMISES, as more fully described in Attachment A (which is incorporated herein by reference), is a white single-family residence. Attachment A also includes a photograph of Decarolis. The evidence described in Attachment B includes evidence maintained in electronic format on any computer (or other device capable of storing data) within the SUBJECT PREMISES. The methods by which the electronic information will be searched are more fully set forth in the “Computer Evidence” section of this affidavit. The items to be seized constitute evidence of the commission of criminal offenses, contraband, fruits of crimes and things otherwise criminally possessed, as well as property designed and intended for use, and that has been used, as a means of committing a crime, namely Production of Child Pornography, in violation of 18 U.S.C. §2251(a), and Possession and Distribution of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) and (a)(2) (the “SUBJECT OFFENSES”).

- b. application under Rule 41 of the Federal Rules of Criminal Procedure, as well as Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to search and seize the following Dropbox, Inc.¹ (“Dropbox”) account, as described more fully in Attachment C, including the contents of communication, associated with email address **boylover1235@yahoo.com** (the “SUBJECT DROPBOX ACCOUNT”). According to government databases, Dropbox accepts service of process at 333 Brannan Street, San Francisco, California 94107 and via the email address legalcompliance@dropbox.com. Dropbox is headquartered at the China Basin Landing Building, 185 Berry Street, Suite 400, San Francisco, California, 94107-1739. The evidence described in Attachment D includes evidence maintained in electronic format within the SUBJECT DROPBOX ACCOUNT. The methods by which the electronic information will be searched are more fully set forth in the “TECHICAL BACKGROUND REGARDING DROPBOX” section of this affidavit; and
- c. application for a search warrant under Title 18, United States Code §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to search and seize the following Snap, Inc. (hereinafter “Snapchat”) account, as described more fully in Attachment E, including the contents of communications, associated with the Snapchat account **rdcarolis3** (the “SUBJECT SNAPCHAT ACCOUNT”) that is stored at premises owned, maintained, controlled, or operated by Snap Inc., a mobile communications provider headquartered at 2772 Donald Douglas Loop North, Santa Monica, California 90405. The evidence described in Attachment F includes evidence maintained in electronic format within the SUBJECT SNAPCHAT ACCOUNT. The methods by which the electronic information will be searched are more fully set forth in the “TECHICAL BACKGROUND REGARDING SNAPCHAT” section of this affidavit.

3. As described herein, there is probable cause to believe that (1) the SUBJECT PREMISES contains evidence of a crime, contraband, fruits of crime, or other items illegally possessed, and property designed for use, intended for use, or used in committing the SUBJECT OFFENSES; (2) violations of the SUBJECT OFFENSES have been committed by the user of the SUBJECT DROPBOX ACCOUNT, and that the content of that account will contain evidence of

¹ Dropbox, Inc. provides remote, “cloud,” or web based, storage of electronic files. Dropbox advertises on its website that users can: “Get to your files from a computer, phone, or tablet,” “Dropbox brings your files together, in one central place. They are easy to find and safely synced across all your devices-so you can access them anytime, anywhere,” “Send files to anyone, even if they don’t have a Dropbox account,” “Dropbox plus lets you share files of any size with just a link,” and “Use shared folders to give everyone simultaneous access to new and updated files.” <https://www.dropbox.com/> (last visited June 12, 2019). Because the files are remotely stored, they are accessible even if one loses the device on which they were originally stored.

a crime; contraband, fruits of crime, or other items illegally possessed; and (3) violations of the SUBJECT OFFENSES have been committed by the user of the SUBJECT SNAPCHAT ACCOUNT, and that the content of that account will contain evidence of a crime; contraband, fruits of crime, or other items illegally possessed.

4. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing the requested search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested search warrants.

STATEMENT OF PROBABLE CAUSE

5. On or about October 25, 2018, HSI's Field Office in Riverside, California ("HSI Riverside") executed a federal search warrant at a residence belonging to an individual located in San Bernardino County, California (the "Riverside Suspect") in furtherance of a child exploitation investigation. The search of the Riverside Suspect's residence resulted in the discovery of child pornography. As a result, the Riverside Suspect was arrested and subsequently charged with violations of 18 U.S.C. § 2251(a) – Production of Child Pornography; 18 U.S.C. § 2252A(a)(2) – Distribution of Child Pornography; and 18 U.S.C. § 2252A(a)(5)(B) – Possession of Child Pornography. During the interview, the Riverside Subject willingly consented to permit HSI agents to assume the Riverside Subject's identity on several online accounts, one of which was the Riverside Subject's Snapchat account (the "Riverside Snapchat").² On or about December 19,

² As described more fully in the Section titled TECHNICAL BACKGROUND REGARDING SNAPCHAT, Snapchat is a multimedia mobile messaging application developed by Snap Inc. One of its principle features is that pictures and messages are usually only available for a short time period before they become inaccessible to their recipients. Multimedia messages are referred to as "snaps", which can consist of photos or short videos that can be sent privately to selected users, or to semi-public "Story" or a public "Story" referred to as "Our Story."

2018, HSI Riverside Special Agent (“SA”) Jonathan Ruiz assumed control of the Riverside Snapchat by changing the password and the phone number to the account. SA Ruiz noticed that there were several active chats on the Riverside Snapchat with other users, including an active chat with a user of the SUBJECT SNAPCHAT ACCOUNT with the account username of “rdecarolis3” and the display name, “Ryan Decarolis.”³ On or about December 25, 2019, SA Ruiz received a message from “Ryan Decarolis” of what appeared to be of himself as Santa Claus with the text of “Merry Christmas” imbedded within the photo. Once SA Ruiz received this message, he was able to see prior saved messages within the chat, including a message on or about August 18, 2018, in which the Riverside Subject sent “Ryan Decarolis” an image of a close-up of the vagina of what appeared to be a prepubescent girl.

6. Based upon the August 18, 2018 receipt of apparent child pornography by “Ryan Decarolis,” in January 2019, HSI Riverside served an administrative subpoena on Snapchat for subscriber information associated with the SUBJECT SNAPCHAT ACCOUNT. On or about January 31, 2019, Snapchat provided the following information in response to the administrative subpoena:

Id: rdecarolis3
 Email address: dechipryan@yahoo.com
 Created: November 4, 2017 at 13:26:58 UTC⁴
 Phone number: (978) 490-0862
 Display name: Ryan Decarolis

7. Between January 29, 2019 to January 30, 2019, the following conversation occurred between the “Ryan Decarolis” and SA Ruiz:

“Ryan Decarolis”: “What u up to”

³ For ease of reference, the user of the SUBJECT SNAPCHAT ACCOUNT will be referred to herein as “Ryan Decarolis,” the Display Name for the account.

⁴ Coordinated Universal Time (“UTC”) is the time standard commonly used across the world. EST is -5 hours.

SA Ruiz: *"Chillin, u?"*

"Ryan Decarolis": *"Same at work"*

SA Ruiz: *"What kind of work again?"*

"Ryan Decarolis": *"Liquor store"*

SA Ruiz: *"That's right"*
"Coo [sic]"
"I need buddies like that"

"Ryan Decarolis": *"Yea I wish I worked around kids though"*

SA Ruiz: *"Best job ever"*
"What would you do"

"Ryan Decarolis": *"Idk but I'd sure have lots of fun 😊"*

8. On or about January 31, 2019, "Ryan Decarolis" sent three images depicting nude, prepubescent female and male children to SA Ruiz at the Riverside Snapchat. One such image depicts two nude, prepubescent females estimated to be between the ages of 5 and 7 years old. Both children are lying on their backs, side-by-side on a bed with their legs slightly spread open; lasciviously displaying their breasts and vaginas. Both children have numbers written on their chest with a white substance that appears to be frosting or shaving cream or similar substance, one child with the number "1" and the other child with the number "8."⁵

9. On or about February 14, 2019, SA Ruiz sent a message to "Ryan Decarolis" asking, *"Are u into boys or girls?" "I forgot."* "Ryan Decarolis" sent a message replying, *"Both just prefer boys."*

10. On or about March 31, 2019, "Ryan Decarolis" sent SA Ruiz a message asking, *"Hey quick question you able to download Dropbox cuz if so I just found my old phone and it's*

⁵ This image is available for the Court's review.

loaded with kids.” Between April 4, 2019 and April 5, 2019, SA Ruiz and “Ryan Decarolis” exchanged several messages, portions of which are as follows:

SA Ruiz:	<i>“Yeah I got Dropbox baby!! What kinda kids though. I don’t trade shit”</i>
”Ryan Decarolis”:	<i>“A little bit of stuff I filmed than a lot girl and boy stuff.”</i>
SA Ruiz:	<i>“Filmed? Like stuff I sent u”</i>
“Ryan Decarolis”:	<i>“No Stuff other” “People have sent”</i>
SA Ruiz:	<i>“Oh. Well what do u film? Was that was u were gonna send me Dropbox?”</i>
”Ryan Decarolis”:	<i>“I was gonna just let u look through my Dropbox”</i>
SA Ruiz:	<i>“Cool! I’m not real familiar with Dropbox but down to see what goodies u got”</i>
”Ryan Decarolis”:	<i>“Ok”</i>
SA Ruiz:	<i>“How u gonna send me the info? Link or email?”</i>
”Ryan Decarolis”:	<i>“I’m gonna give u the login”</i>

11. On or about April 5, 2019, “Ryan Decarolis” sent a message to SA Ruiz providing “boylover1235@yahoo.com” as a login name and password of “Redsox209” for his Dropbox account (the “SUBJECT DROPBOX ACCOUNT”). During the same chat conversation, SA Ruiz sent a message to “Ryan Decarolis” asking *“It’s urs [sic] and NOT someone else’s right”* (referring to the SUBJECT DROPBOX ACCOUNT), and “Ryan Decarolis” responded, *“It’s all stuff people sent me and some of mine.”* SA Ruiz replied clarifying, *“But ur [sic] account I mean. Don’t want to log into something that a cop gave u [sic] trying to pretend he’s cool.” “Know what I mean?”* “Ryan Decarolis” replied, *“Its mine.”* The Dropbox account provided to SA Ruiz is

registered to and identified by the email address, “boylover1235@yahoo.com”.⁶ SA RUIZ sent a message to “Ryan Decarolis” asking if he could save some videos from the SUBJECT DROPBOX ACCOUNT. “Ryan Decarolis” replied by sending a message stating, “*Help ur self.*” On the same day, SA Ruiz successfully accessed the SUBJECT DROPBOX ACCOUNT on three occasions by using the email address and password provided by “Ryan Decarolis.” SA RUIZ successfully download the contents of the SUBJECT DROPBOX ACCOUNT and captured certain account information, including the email associated with the account (“boylover1235@yahoo.com”) and the name on the account (“Fbbu lgyz”) from the “General” section of the SUBJECT DROPBOX ACCOUNT.

12. After reviewing some of the photographs contained in the SUBJECT DROPBOX ACCOUNT, SA Ruiz observed a non-pornographic photograph depicting DECAROLIS alongside a minor-aged, male child, which will be described in greater detail below.⁷ Referring to this photograph, SA Ruiz sent a message to “Ryan Decarolis” asking, “*Whose the little black boy with u in the pic. Do anything with?*” “Ryan Decarolis” sent two messages responding, “*Just sucked*” and “*Ex friend kid.*” SA Ruiz sent a message asking, “*He’s cute. U [sic] sucked him or he sucked u? Both?*” “Ryan Decarolis” responded, “*I sucked him.*”

13. I reviewed the contents of the SUBJECT DROPBOX ACCOUNT,⁸ downloaded by SA Ruiz, and found the account to contain at least 250 video and image files that appear to contain

⁶ As described more fully in the Section titled TECHICAL BACKGROUND REGARDING DROPBOX, Dropbox is a file hosting service operated by Dropbox, Inc., headquartered San Francisco, California, that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox users sign up for an account with a valid e-mail address. Dropbox will typically give users a certain amount of free storage, and if the user wants more storage, the user can pay for it.

⁷ I was able to ascertain that the adult male depicted in this picture and other photographs in the SUBJECT DROPBOX ACCOUNT to be Ryan DECAROLIS from a comparison of photographs from his Massachusetts driver’s license and his Facebook account.

⁸ Given Dropbox’s policy of disclosing subpoenas to account holders, I did not serve an administrative subpoena on Dropbox for subscriber information associated with the SUBJECT DROPBOX ACCOUNT.

child pornography. The files, a mix of pictures and videos, depicted mostly prepubescent boys engaged in sexual conduct with children and adults. The apparent child pornography were contained in several folders. One such file, “d7ba5990-a055-43fd-b418-6d24bddd4279.mp4”, was located in the folder labeled “H” in the subfolder labeled “001”. The video is approximately 1 minute and 57 seconds in length and depicts a prepubescent, nude female child that appeared to be 1 to 2 years old lying on her back with her breasts and vagina lasciviously exposed. In this video, the child is seen being anally penetrated by an adult’s finger. Later in the video, an adult’s hand is seen rubbing the child’s vagina.⁹

14. I reviewed another file that was downloaded from the SUBJECT DROPBOX ACCOUNT by SA Ruiz titled “Photo Feb. 23, 10 10 37 PM.jpeg.” This file is an image that appeared to depict DECAROLIS wearing a Boston Red Sox baseball hat. This file also contained metadata information including the make and model of the device that took the picture; date and time on when the photograph was taken and the location coordinates of where the picture was taken.¹⁰ Using available online software, I was able to view the metadata for this file and determine that this photo was taken February 23, 2017 at approximately 10:10 PM using an iPhone 6s Plus. According to the GPS coordinates, this picture was taken at a location in Fitchburg, Massachusetts.

15. I also reviewed the file of the non-pornographic image of DECAROLIS with a male child approximately 3 to 5 years old titled, “Photo Feb 23, 10 11 49 PM. jpeg.” This is the photo SA Ruiz was referring to during a chat conversation with DECARLOIS, described above in Paragraph 12. Metadata for this image indicates that the image was taken on February 23, 2017

⁹ A still image from this video is available for the Court’s review.

¹⁰ Metadata describe other data and provides information about certain item’s content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document’s metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.

at approximately 10:11 PM using an iPhone 6s Plus at a location in Leominster, Massachusetts, approximately one minute after and a half mile away from the photograph of DECAROLIS described in Paragraph 14.

16. Also contained in the SUBJECT DROPBOX ACCOUNT was a file titled “Photo Apr 09, 1 35 33 AM.jpeg,” which is an image depicting a close-up of a prepubescent, penis of child approximately between 3 and 5 years old. In this image, an adult hand is seen pulling down the child’s clothing causing the child’s genital to be exposed. The child’s face and other portions of his body, besides the boy’s penis, are not depicted in this photo.¹¹ Metadata for this file indicated that it was taken April 09, 2017 using an iPhone 6s Plus in Worcester, Massachusetts.

17. On or about May 3, 2019, HSI Boston served an administrative subpoena to Yahoo! for subscriber information for “boylover1235@yahoo.com,” the email address associated with the SUBJECT DROPBOX ACCOUNT, as well as “dechipryan@yahoo.com, the email address associated with the SUBJECT SNAPCHAT ACCOUNT. On or about May 15, 2019, Yahoo! provided the following information in response to the administrative subpoena:

Yahoo Mail Name: boylover1235@yahoo.com
Account Creation: March 7, 2017
Alternate Communication Channels: dechipryan@yahoo.com (*unverified*)
(978) 490-0862 (*verified*)

Yahoo Mail Name: dechipryan@yahoo.com
Account Creation: April 29, 2012
Alternate Communication Channels: (978) 490-0862 (*verified*)

18. On the same day, HSI Boston served an administrative subpoena on Sprint Corporation (“Sprint”) for subscriber information for telephone number, (978) 490-0862, the telephone number associated with the “boylover1235@yahoo.com” and

¹¹ This image is available for the Court’s review.

“dechipryan@yahoo.com” email addresses and the SUBJECT SNAPCHAT ACCOUNT. On or about May 15, 2019, Sprint provided the following information in response to the administrative subpoena:

Account Number: 438115771
Name: Ryan Decarolis
Address: 12 Clifton Street, Fitchburg, Massachusetts 01420

19. In response to the May 3, 2019 administrative subpoena, Yahoo! also provided Internet Protocol (“IP”) addresses¹² used to login to the “boylover1235@yahoo.com” and “dechipryan@yahoo.com” email accounts. The same IP address, 73.126.127.163, was used to login into “boylover1235@yahoo.com” on March 25, 2019 at 20:40 GMT¹³ and into “dechipryan@yahoo.com” on April 17, 2019 at 8:19 GMT. In addition, IP address 2600:0001:f566:969d:f9ee:8b30:2c72:7335 was utilized to login into “dechipryan@yahoo.com” on April 8, 2109 at 7:32 GMT.

20. A search of the American Registry of Internet Numbers (“ARIN”) revealed that IP address 73.126.127.163 is registered to Comcast Cable Communications (“Comcast”). A search of ARIN revealed that IP address 2600:0001:f566:969d:f9ee:8b30:2c72:7335 is registered to Sprint Corporation (“Sprint”).

21. On or about June 24, 2019, HSI Boston served an administrative subpoena to Comcast to provide subscriber information for IP address 73.126.127.163 on the dates and times that it was used to login into the “boylover1235@yahoo.com” and “dechipryan@yahoo.com”

¹² An Internet Protocol (“IP”) address refers to a unique numerical value assigned to a computer or mobile device when it is connected to the Internet.

¹³ GMT refers to Greenwich Mean Time, which marks the starting point of every time zone of the time zone map. EST is -4 hours.

email addresses, as described in Paragraph 19 above. On or about June 25, 2019, Comcast provided the following information in response to the administrative subpoena:¹⁴

Name: David Decarolis
Service Address: 12 Clifton St., Fitchburg, MA 01420
Telephone: (978) 342-****
Type of Service: High Speed Internet Service
Account #: 8773103500819750
Account Status: Active

22. On or about June 24, 2109, HSI Boston served an administrative subpoena on Sprint to provide subscriber information for IP address 2600:0001:f566:969d:f9ee:8b30:2c72:7335 on the date and time it was used to login into the “dechipryan@yahoo.com” email, as described in Paragraph 19 above. On or about July 2, 2019, Sprint responded that this IP address resolved to DECAROLIS’ Sprint account, as described in Paragraph 18.¹⁵

23. According to the City of Fitchburg Assessor’s database, the owners of the SUBJECT PREMISES are David and Donna Decarolis, who are believed to be DECAROLIS’ parents.

24. From a review of records held by the Massachusetts Registry of Motor Vehicle (“MA RMV”), I learned that DECAROLIS has a Massachusetts Identification Card that lists the SUBJECT PREMISES as his residential address. Furthermore, MA RMV records indicate that David Decarolis (YOB: 1964) and Donna Decarolis (YOB: 1962) listed the SUBJECT PREMISES as their residential address on their driver’s licenses and on active and previous vehicle registrations.

¹⁴ Six additional IP addresses connected to the “boylover1235@yahoo.com” and “dechipryan@yahoo.com” email addresses were included in the administrative subpoena to Comcast and determined to resolve to the same Comcast account.

¹⁵ Another IP address connected to the “dechipryan@yahoo.com” email was included in the administrative summons to Sprint, which was determined to resolve to the same Sprint account.

25. On or about July 26, 2019, members of the Fitchburg Police Department (“FPD”) went the SUBJECT PREMISES and made contact with its occupants. Under the guise of a ruse, FPD encountered DECAROLIS who answered the door and confirmed that he currently resides at the SUBJECT PREMISES.

26. On July 29, 2019, utilizing a wireless device, I conducted a search of the wireless networks in the vicinity of the SUBJECT PREMISES, which revealed that all of the wireless networks observed were secured or password-protected and not open for public.

Characteristics Common to Individuals who Consume Child Pornography

27. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web-based services to access with intent to view and possess, collect, receive, or distribute images of child pornography (*i.e.*, consumers of child pornography), as follows:

- a. Consumers of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media.
- b. Consumers of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, videos, books, drawings, other visual media, and, increasingly, digital format. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Consumers of child pornography almost always possess and maintain their child pornographic material (whether stored in hard copy or digitally) in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, videos, digital media, and other documentation of child pornography and child erotica for many years.¹⁶

¹⁶ See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child

Such individuals often maintain their digital or electronic child pornography in a safe, secure, and private environment, such as a computer, phone and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are highly valued by them. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

- d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and other digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.¹⁷
- e. Consumers of child pornography also may correspond with and/or meet others to share information and materials; often maintain correspondence from other child pornography consumers; conceal such correspondence as they do their sexually explicit material; and often maintain the contact information of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Consumers of child pornography prefer not to be without access to child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

28. Based upon all of the foregoing, I submit that there is probable cause to believe that DECAROLIS is a possessor, distributor and producer of child pornography who possessed images of child pornography on his computer and distributed them by providing his Dropbox login credentials (username and password) to SA Ruiz on or about April 5, 2019. As a possessor and distributor of child pornography, DECAROLIS likely places great value on these images and maintains them on his computer or other data storage device in his home to this day. Given the

pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

¹⁷ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

propensity of possessors and distributors to store such images within the privacy of their own homes, there is probable cause to believe that DECAROLIS currently maintains these images on a computer or other data storage device located within the SUBJECT PREMISES.

Search and Seizure of Computer Systems and Data

29. As set forth above, probable cause exists to believe that the SUBJECT OFFENSES were perpetrated through the use of computer equipment capable of accessing the internet.

30. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

31. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media (“computer equipment”) be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

- a. The volume of evidence — storage media such as hard disks, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements — analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

32. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

33. The SUBJECT PREMISES may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s

knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine its true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

TECHNICAL BACKGROUND REGARDING DROPBOX

34. Dropbox, a Remote Computer Services Provider,¹⁸ is a file hosting service operated by Dropbox, Inc., headquartered in San Francisco, California, that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications.

35. Dropbox users sign up for an account with a valid e-mail address. To sign into the user's Dropbox account, the user enters an email address and password. Dropbox will typically give users a certain amount of free storage, and if the user wants more storage, the user can pay for it. Users can access Dropbox from anywhere in the world using the internet and avoid having the files appear on the user's computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted to store them at an offsite location such as Dropbox. For example, a user can take a photograph from a smartphone and upload that photo to Dropbox and erase it from their phone. The photograph

¹⁸ As defined by 18 U.S.C §2711, "the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system."

now resides in the user's "cloud." The user can then access his/her Dropbox account from a desktop computer and download the photograph to that machine.

36. Dropbox provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information ("PII"), which can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email address(es), and means and source of payment, including any credit or bank account number (for paying customers).

37. Another feature of Dropbox is sharing. A Dropbox user can share certain files he/she designates by sending a web link to another user. It then gives the second user access to those particular files.

38. I know that Dropbox maintains records on their users, such as basic subscriber information within the meaning of 18 USC 2703(c)(2). Furthermore, I know Dropbox keeps and maintains the stored content of their users' accounts, such as photographs, movies, documents, and music, all within the meaning of the Stored Communication Act.

39. According to Dropbox's privacy policy, at <https://www.dropbox.com/privacy> (last visited June 14, 2019), Dropbox collects and stores:

"[user's] name, email address, phone number, payment info, and physical address;"

"[user's] files, documents, photos, comments, messages, and so on;"

"things like the size of the file, the time it was uploaded, collaborators, and usage activity...like sharing, editing, viewing, and moving files or folders;"

“Information from and about the devices...use[d] to access the Services...like IP addresses, the type of browser and device...use[d], the web page...visited before coming to our sites, and identifiers associated with [user’s] device.”

40. Based on my training and experience, I know that electronic communication services and remote computing services such as Dropbox Inc. retain business records and subscriber information such as account applications, subscribers’ full names, all screen names associated with the subscribers and/or account, all account names associated with the subscribers, services available to the subscriber, methods of payment, telephone numbers, addresses, passwords, and detailed billing records.

41. Based on my training and experience, I also know that electronic communication services and remote computing services such as Dropbox Inc. maintain electronic records pertaining to the individuals and companies for whom they maintain subscriber accounts including account access information, email transaction information, and account application information, email communications, and image files.

42. Through my training and experience, I know that private citizens and businesses are using electronic service providers (“ESPs”) who provide the service of storing data from anywhere there is a connection to the internet, commonly known as cloud based storage. This allows the customer to connect to the server and view, alter, create, copy, and print the data from the remote server as if it was at the same location as the user. The user typically owns and controls the data stored at the remote server while the ESP owns the server on which the data is stored.

43. As in the instant case, law enforcement typically does not find out about the existence of the remote server. Law enforcement cannot access or view this cloud-based data unless they know it exists and have access to a remote computer capable of connecting to and

authenticating the user's cloud-based account. Witnesses and informants who have access to the data also typically do not know where the data is stored.

44. The server may be located in another city or state from the site of the initial service, making it difficult for law enforcement to preserve the evidence in a traditional manner. It takes hours and sometimes days to determine the location of the remote server and gather the details containing the specificity necessary for the issuance of a second search warrant. Depending on the size of the evidence, a suspect can delete it from a system within seconds using a smart phone or another internet capable device at any location. A forensic examiner often can recover evidence suggesting whether a computer (including a computer, cell phone, tablet, or other internet capable device) was used to access data which had been stored on a remote server in a cloud storage account. Such information is often maintained indefinitely until overwritten by other data.

45. Based upon the initial review of the content of the SUBJECT DROPBOX ACCOUNT, I sent Dropbox, Inc. a letter on July 24, 2019, requesting under 18 U.S.C § 2703(f) that the company preserve records associated with the SUBJECT DROPBOX ACCOUNT for a period of 90 days.

46. In general, content that is sent to a Dropbox account is stored in the subscriber's "user account" on Dropbox servers until the subscriber deletes the content. If the subscriber does not delete the content, the content can remain on Dropbox's servers indefinitely. Even if the subscriber deletes the content, it may continue to be available on Dropbox's servers for a certain period of time.

47. In my training and experience, I have learned that Dropbox provides a "cloud" based storage service to the public. Given Dropbox's subscription practices, Dropbox's computers are likely to contain stored data (including photographs, videos, documents,

applications, music, and other content) and information concerning subscribers and their use of Dropbox services, such as account access information, registration email account, and account application information. In my training and experience, such information may constitute evidence of a crime under investigation because the information can be used to identify the account user and images and videos contained within the account may contain child pornography.

48. In my training and experience, cloud storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as IP addresses from which the account was accessed and/or registered), and other log files that reflect usage of the account. Because every device utilizes an IP address to connect to the internet, IP address information can help identify which computers or devices were used to access the Dropbox account.

49. Based on my training and experience, I also know the following:

- a. People who have a history of and interest in sexual encounters with children will likely collect sexually explicit and suggestive material consisting of photographs, videos, and visual depictions of minors with whom they have had sexual contact and of other minors who stimulate their own sexual gratification, and they are likely to have these materials in their possession and/or stored in their email or online accounts.
- b. People who have a history of and interest in sexual encounters with children will likely have records detailing communications with minors and other correspondence (with minors or adults) or records discussing sexual activity involving minors.
- c. People who collect child pornography almost always store these images on computers and other computer equipment, including web-based storage, and storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Such persons rarely, if ever, dispose

of their sexually explicit materials, especially when they themselves have taken the photographs or made the videos, as these materials are considered prized possessions.

TECHNICAL BACKGROUND REGARDING SNAPCHAT

50. In my review of the Snapchat Law Enforcement Guide and other law enforcement resources, I have learned that Snapchat is a free-access social networking mobile application made by Snap, Inc. The application is available through the Apple iPhone app store and Google Play and provides users a way to share photos, videos and text. Snapchat is one of the most popular applications for sending and receiving ‘self-destructing’ messages, pictures, and videos, referred to as “snaps.” The company processes approximately 700 million snaps every day. Snapchat users access the application frequently. According to marketing material provided by the company, the average Snapchat user checks their account 14 times per day.

51. Subscribers obtain an account by downloading the free Snapchat application to their mobile media device and registering an account with Snapchat. During the registration process, Snapchat asks subscribers to provide basic personal information including email address and phone number. The phone number is verified during the registration process. When registering a Snapchat account, an individual must select a username. The username is a unique identifier associated with the account and cannot be changed by the user once selected. A user can also select a display name, which is not a unique identifier.

52. Snapchat collects and maintains basic subscriber information when a user creates a new Snapchat account, alters information at a later date, or otherwise interacts with the Snapchat application. Basic subscriber information may include: Snapchat username, email address, phone number, display name, Snapchat account creation date and IP address, and timestamp and IP address of account logins and logouts. The basic subscriber information entered by a user in

creating an account is maintained as long as the user has not edited the information or removed the information from the account.

53. Snapchat users can take photos or video “Snaps” using the camera on their cellular device. A “Snap” is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long a Snap can be viewed. Once a Snap has been viewed it is deleted from the company’s system and is no longer visible to the recipient. In addition, Snapchat users can send pictures to other users from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and “Snaps” constitutes “electronic communications” within the meaning of 18 U.S.C. § 3123. See 18 U.S.C. §§ 3127(1) and 2510(12).

54. A user can add snaps to their “Story.” A Story is a collection of Snaps displayed in chronological order. Each Snap in a “Story” documents the user’s experience. Based on the user’s privacy settings, the photos and videos added to a “Story” can be viewed either by everyone on Snapchat or just the user’s friends. “Our Stories” is a collection of user-submitted “Snaps” from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of Snaps regarding the event. Stories are visible to other users for up to 24 hours.

55. “Memories” is Snapchat’s cloud-storage service, where users can save their sent or unsent Snaps, posted stories, photos, and videos from their phone’s photo gallery. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, photos, and videos saved in Memories are backed up by Snap Inc. and may remain in Memories until deleted by the user.

56. Another feature available to Snapchat users is the “Chat” feature. A user can type messages and send photos, videos, audio notes, and video notes to friends within the Snapchat

application. Once a chat message is viewed by both the sender and the recipient, and both parties swipe away from the chat screen, the message will be cleared. Within the Snapchat application itself, a user can opt to save part of the chat by tapping on the message that they want to keep. The user can clear the message by tapping it a second time.

57. If Snapchat users have device-level location services turned on and have opted into location services on the application, Snapchat will collect location data at various points during their use of Snapchat. The “Snap Map” feature allows users to see where their friends are, as long as these friends choose to share their locations. Location sharing with friends via Snap Map is optional. If a user submits a Snap to “Our Story” it may appear publicly on the Map in the exact location it was taken.

58. Snapchat retains logs for Snaps for thirty days. Logs for posted Stories are retained for 24 hours or until deleted by the user. Chat content will be available only if the sender or the recipient chooses to save the Chat, or if the Chat is unopened (within thirty days of sending). Memories may be available until deleted by the user.

59. While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

60. Based on my training and experience, I am aware that companies that host social-networking accounts, and Snapchat in particular, generally maintain records of their subscribers’ online activities and private communications unless the user deletes these communications.

61. On July 24, 2019, I sent Snapchat a letter requesting under 18 U.S.C § 2703(f) that the company preserve records associated with the SUBJECT SNAPCHAT ACCOUNT for a period of 90 days.

LEGAL AUTHORITY

62. The government may obtain both electronic communications and subscriber information from a provider of electronic communication services and remote computing services by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A). For this remainder of this Affidavit, I refer to both Dropbox and Snap, Inc. as the Electronic Providers.

63. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by Title 18, United States Code, Sections 2711, 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). Specifically, the Court is “a district court of the United States...that – has jurisdiction over the offense being investigated,” Title 18, United States Code, Section 2711(3)(A)(i). Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g). If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

64. Because the warrants will be served on the Electronic Providers who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

65. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Section 2703(a), 2703(b)(1)(A) and

2703(c)(1)(A), by using the warrant to require the Electronic Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachments D (for Dropbox) and F (for Snapchat), Upon receipt of the information described in Attachments D and F, government-authorized persons will review that information to locate the items described in Attachments D and F.

66. This application seeks warrants to search all responsive records and information under the control of the Electronic Providers, providers subject to the jurisdiction of this court, regardless of where the Electronic Providers have chosen to store such information. Pursuant to Title 18, United States Code, Section 2713, the government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within the Electronic Providers' possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside of the United States.¹⁹

67. Because voluminous amounts of information can be stored in a cloud storage account, and because it might be stored in a deceptive order or with deceptive file names to conceal criminal activity, the searching authorities must examine all the stored data to determine which files constitute evidence, fruits, or instrumentalities of the crime. This sorting process can be very time-

¹⁹ It is possible that the Electronic Providers store some portion of the information sought outside of the United States. In *Microsoft Corp. v. United States*, 829 F.3d 197 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, and as two courts have more recently held that the government *can* compel the production of foreign-stored data, *see In re: Information Associated with one Yahoo email address that is stored at premises controlled by Yahoo*, 2017 WL 706307 (E.D. Wisc. Feb. 21, 2017) & *In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017), I respectfully request that this warrant apply to all responsive information – including data stored outside the United States – pertaining to the identified account that is in the possession, custody, or control of the Electronic Providers. The government also seeks the disclosure of the physical location or locations where the information is stored.

consuming and would be impractical to do at either of the Electronic Provider's offices. Moreover, the sorting process should be done in a controlled environment because of the vast array of computer hardware and software that might be necessary even for computer experts to analyze the data, in order to insure the integrity of the data recovered. Therefore, I request authority to seize all content and other records as more fully set forth in Attachments D (for Dropbox) and F (for Snapchat), including any attached files, and other communications stored in this account, to be searched off site.

REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBER(S)

68. I request that these applications, the warrants, the orders, and any related papers be sealed by the Court until such time as the Court pursuant to Local Rule 7.2 directs otherwise.

69. I further request that, pursuant to 18 U.S.C. §§ 2705(b) and 2703(b)(1)(A), the Court order the Electronic Providers not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, the Order, or the execution of the warrant for the earlier of one year from the date of the court's order or upon notice by the government within 30 days of the conclusion of its investigation, unless the court extends such period under Title 18, United States Code, Section 2705(b). Non-disclosure is appropriate in this case because the court's order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the existence of the investigation. Accordingly, there is reason to believe that notification of the existence of the order will seriously jeopardize the investigation, including by giving targets an opportunity to flee prosecution, destroy or tamper with evidence, change patterns of behavior, or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b). Moreover, some of the evidence in this investigation is stored electronically. If alerted to the existence of the order, the targets could destroy that evidence, including

information saved to their personal computing devices, on other electronic media, or in social media accounts.

FOURTEEN DAY RULE FOR EXECUTION OF WARRANT

70. Federal Rules of Criminal Procedure 41(e)(2)(A) and (B) direct the United States to execute a search warrant for electronic evidence within fourteen (14) days of the warrant's issuance. If the Court issues this warrant, the United States will execute them not by entering the premises of the Electronic Providers, as with a conventional warrant, but rather by serving a copy of the warrant on the respective companies and awaiting their production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto internet companies' physical premises and the resulting disruption of their business practices.

71. Based on the training and experience of myself and other law enforcement agents, I understand that electronic account providers sometimes produce data in response to a search warrant outside the 14-day (formerly 10-day) period set forth in Rule 41 for execution of a warrant. I also understand that electronic account providers sometimes produce data that was created or received after this 14-day deadline ("late-created data"). The United States does not ask for this extra data or participate in its production.

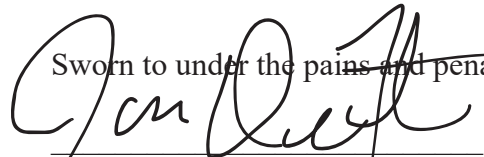
72. Should the Electronic Providers produce late-created data in response to this warrant, I request permission to view all late-created data that was created by the Electronic Providers, including subscriber, IP address, log records, and other transactional data, without a further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as messages, absent a follow-up warrant.

73. For these reasons, I request that the Court approve the procedures in Attachment D associated with the SUBJECT DROPBOX ACCOUNT, and Attachment F associated with the SUBJECT SNAPCHAT ACCOUNT which set forth these limitations.


CONCLUSION

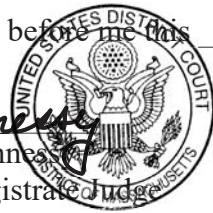
74. Based on all of the foregoing, I submit that there is probable cause to believe that (1) evidence of the commission of criminal offenses, contraband, fruits of crimes and things otherwise criminally possessed, as well as property designed and intended for use, and that has been used, as a means of committing the "SUBJECT OFFENSES", as described in Attachment B, are located at the SUBJECT PREMISES, or on the person of DECAROLIS, as more fully described in Attachment A; (2) the SUBJECT DROPBOX ACCOUNT contains evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES; and (3) the SUBJECT SNAPCHAT ACCOUNT contains evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES, and request that the Court issue the requested search warrants.

Sworn to under the pains and penalties of perjury,


Special Agent Jason J. DeFreitas
Homeland Security Investigations

Subscribed and sworn to before me this 1st day of ~~July~~ ^{August}, 2019.


Honorable David H. Hennessey
Chief United States Magistrate Judge



I have reviewed still images from the videos referenced in Paragraphs 8, 13, and 16 above and I find probable cause to believe that they depict minors engaged in sexually explicit conduct. The affiant shall preserve the images provided to the Court for the duration of the pendency of this matter, including any relevant appellate process.


Honorable David H. Hennessey
Chief United States Magistrate Judge

